

FILED IN CLERK'S OFFICE
U.S.D.C. - Atlanta

SEP 08 2017

JAMES N. HATTEN, Clerk
By:  Deputy Clerk

David J. Maher
Rodney K. Strong
GRIFFIN & STRONG, P.C.
235 Peachtree Street N.E., Suite 400
Atlanta, GA 30303
Phone: 404-584-9777
Fax: 404-584-9730

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA**

Joseph M. Kuss

Plaintiff

v.

Equifax, Inc.

Defendant

Case No.: **1:17-CV-3436**

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiffs Joseph M. Kuss and Stacy Markowitz ("Plaintiff" or Plaintiffs"), individually and on behalf of all others similarly situated, based on personal knowledge as to their own experiences and on investigation of counsel as to all other matters, alleges the following against Defendant Equifax, Inc. ("Equifax" or "Defendant").

INTRODUCTION

1. Plaintiffs bring this action, individually and on behalf of all others similarly situated whose personal and non-public information—including names, Social Security numbers, birth dates, addresses, driver’s license numbers, and credit report histories (collectively, “Confidential Information”)—was compromised in a massive security breach of Defendant Equifax, Inc.’s (“Defendant” or “Equifax”) computer servers beginning in May 2017 and lasting through July 2017 (the “Data Breach”).

2. As alleged herein, the injuries to Plaintiffs and the Class were directly and proximately caused by Defendant’s failure to implement or maintain adequate data security measures for consumers’ information including Confidential Information.

3. Defendant failed to take reasonable steps to employ adequate security measures or to properly protect Confidential Information despite two similar cyber security breaches to its own system within the last two years.

4. The most recent Data Breach at Equifax was the inevitable result of its inadequate data security measures and approach to data security. Despite the well-publicized and ever-growing threat of security breaches involving Confidential Information, and despite that these types of data breaches were and are occurring throughout the restaurant and retail industries, Equifax failed to ensure that it maintained adequate data security measures, failed to implement best practices, failed to upgrade its security systems, and failed to comply with industry standards by allowing its computer and point-of-sale systems to be hacked, causing Confidential Information entrusted to it to be stolen.

JURISDICTION AND VENUE

5. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds \$5 million, exclusive of interest and costs, and is a class action in which some members of the Class are citizens of states different than Defendant. *See* 28 U.S.C. § 1332(d)(2)(A). This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

6. This Court has personal jurisdiction over Defendant. Defendant has sufficient minimum contacts with the state of Georgia because it incorporated in and has its principal place of business in Georgia and because it intentionally avails itself of the consumers and markets within Georgia through the promotion, marketing, and sale of its food services.

7. Venue properly lies in this district pursuant to 28 U.S.C. § 1391(a)(2) because Defendant conducts substantial business in this district, is incorporated in Georgia, headquartered in this district, and is deemed to be a citizen of this District. A substantial part of the events and/or omissions giving rise to the claims occurred, in part, within this District.

PARTIES

Plaintiff Joseph M. Kuss

8. Plaintiff Kuss is a citizen of the state of Delaware and currently resides in Middletown, Delaware.

9. In early August 2017, while attempting to use Equifax's online tools, Plaintiff Kuss noticed that they were unavailable for a number of days.

10. On September 7, 2017, Plaintiff Kuss learned from news reports about the Equifax Data Breach, and he was concerned that his Confidential Information had been compromised.

11. On September 8, 2017, Equifax provided an online resource to discover whether an individual consumer's information had been compromised. Plaintiff Kuss went online and used the resource to discern whether his Confidential Information had been compromised in the Data Breach.

12. The Equifax resource stated that Plaintiff Kuss's information had been compromised:

Thank You

Based on the information provided, we believe that your personal information may have been impacted by this incident.

Click the button below to continue your enrollment in TrustedID Premier.



For more information visit the FAQ page.

13. Plaintiff Kuss expected that his Confidential Information would remain private.

14. Plaintiff Kuss now faces an increased likelihood that his compromised information will lead to identity theft and credit report issues. Plaintiff Kuss may have to spend a substantial amount of time correcting any fallout from this Data Breach. As a result of Defendant's conduct, Kuss has been injured.

Plaintiff Stacy Markowitz

15. Plaintiff Markowitz is a citizen of the Commonwealth of Pennsylvania and currently resides in Exton, Pennsylvania.

16. On September 8, 2017, Plaintiff Markowitz learned from news reports about the Equifax Data Breach, and he was concerned that her Confidential Information had been compromised.

17. Like Plaintiff Kuss, the Equifax resource stated that Ms. Markowitz' information had been compromised.

18. Plaintiff Markowitz expected that her Confidential Information would remain private.

19. Plaintiff Markowitz now faces an increased likelihood that her compromised information will lead to identity theft and credit report issues. Plaintiff Markowitz may have to spend a substantial amount of time correcting any fallout from this Data Breach. As a result of Defendant's conduct, Ms. Markowitz has been injured.

Defendant Equifax, Inc.

20. Defendant is a corporation incorporated under the laws of Georgia. Defendant has its principal place of business at 1550 Peachtree Street, N.W., Atlanta, Georgia. Equifax is one of the three major credit reporting companies in the United States. Equifax is a multi-billion dollar company that tracks consumers' credit histories by gathering information from, among others, banking institutions, credit card companies, and retailers.

FACTUAL ALLEGATIONS

21. Equifax collects a broad range of information regarding consumers' credit. It collects all information relevant to identifying individuals and their credit and spending habits. It collects this information from, among others, banking institutions, retailers, and credit card companies. This information includes highly sensitive data such as the Confidential Information,

which, if it falls into the wrong hands, can be used for nefarious purposes. Indeed, cybersecurity professionals call this a “treasure trove” and “the Crown Jewel” of stolen information.

22. Equifax collects this information regarding most Americans that have credit. Many consumers are unaware that Equifax collects Confidential Information about them.

23. Equifax then uses this information to synthesize a credit history and a credit score for individual consumers. Equifax also uses Confidential Information to sell and market various products and, thus, derives a benefit from it.

24. Confidential Information is not publicly accessible data. Like Plaintiff, consumers do not expect that others have ready access to the Confidential Information. Consumers expect that it is private and securely held.

25. Equifax stores this Confidential Information on its computer server systems. The systems are linked to the internet. At all relevant times, Equifax was aware of the importance of safeguarding consumers’ Confidential Information.

26. Despite its earlier knowledge of the Data Breach, Equifax released a statement disclosing the Data Breach on September 7, 2017. In the general statement, Equifax disclosed that internet hackers breached Equifax’s computer system. Equifax stated that the Data Breach impacted 143 million U.S. consumers. The hackers gained access to Equifax’s giant database containing consumers’ Confidential Information.

27. The hackers stole Confidential Information. This information can be used to impersonate the consumers (identity theft), access their bank accounts, and destroy their credit histories and scores.

28. Anyone who gains access to Confidential Information can impersonate the consumer because financial institutions, creditors, and service providers rely on this information

to identify the consumer. Based on this information, the credit services also make critical financial decisions regarding this consumer, *e.g.*, whether they are approved for a mortgage loan, credit, etc.

29. Consumers that have their Confidential Information stolen suffer from an increased chance that they will fall victim to identity theft. Identity theft results in a significant loss of money and time to resolving discrepancies in expenditures and credit reports.

30. Equifax is providing consumers with a one-year protection service, but it is woefully inadequate. Hackers sell or trade Confidential Information on the internet. The information, however, may not be sold or used within the year especially considering the influx of stolen information from this Data Breach. Hackers may sit on the information and wait out the one-year protection and then sell it.

31. This is the second time in two years that Equifax's cybersecurity measures have proved inadequate to safeguard its vast database of consumers' Confidential Information.

32. Equifax's cybersecurity measures were inadequate to protect the vast amount of information it collects on virtually all American consumers. Equifax had a duty to maintain reasonable and safe cybersecurity measures to protect consumers' Confidential Information.

CLASS ACTION ALLEGATIONS

33. Plaintiffs bring this action on his own behalf, and on behalf of the following Class pursuant to FED. R. CIV. P. 23:

All consumers whose Confidential Information was compromised by the Equifax Data Breach between May 2017 and July 2017.

34. Excluded from the Class are Defendant, its affiliates, officers, directors, assigns, successors, and the Judge(s) assigned to this case. Plaintiff reserves the right to modify, change, or expand the definitions of the Class based on discovery and further investigation.

35. **Numerosity**: While the precise number of Class members has not yet been determined, members of the Class are so numerous that their individual joinder is impracticable, as the proposed Class appears to include, at least, 143 million members who are geographically dispersed.

36. **Typicality**: Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all members of the Class were injured through Equifax's uniform misconduct. The same event and conduct that gave rise to Plaintiffs' claims are identical to those that give rise to the claims of every other Class member because Plaintiffs and each member of the Class had their Confidential Information compromised in the same way by the same conduct by Equifax.

37. **Adequacy**: Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the Class that they seek to represent; Plaintiffs have retained counsel competent and highly experienced in class-action litigation; and Plaintiffs and their counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and his counsel.

38. **Superiority**: A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the Class individually to effectively redress Defendant's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the

class-action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

39. **Existence and Predominance of Common Questions of Fact and Law:**

Common questions of law and fact exist as to all members of the Class. These questions predominate over the questions affecting individual Class members. These common legal and factual questions include, but are not limited to, the following:

- whether Equifax engaged in the wrongful conduct alleged herein;
- whether Equifax owed a duty to Plaintiffs and members of the Class to adequately protect their Confidential Information and to provide timely and accurate notice of the data breach to Plaintiffs and the Class;
- whether Equifax breached its duty to Plaintiffs and the Class by failing to provide timely and accurate notice to Plaintiffs and the Class about the breach;
- whether Equifax breached duties owed to Plaintiffs and the Class by failing to provide adequate data security;
- whether Equifax violated federal and state laws, thereby breaching its duties to Plaintiffs and the Class;
- whether Equifax knew or should have known that its computer and network systems were vulnerable to attack from hackers;
- whether Equifax's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its computer and network systems, resulting in the loss of consumers' Confidential Information;
- whether Equifax wrongfully failed to inform Plaintiffs and members of the Class that it did not maintain computer software and other security procedures sufficient

to reasonably safeguard consumer financial and personal data; and whether Equifax failed to inform Plaintiffs and the Class of the data breach in a timely and accurate manner;

- whether Equifax wrongfully waited to inform Plaintiffs and Class members that their sensitive financial and personal information was exposed in the security breach;
- whether Equifax continues to breach duties to Plaintiffs and Class members and continues to fail to adequately protect sensitive Confidential Information and other financial information;
- whether Equifax has sufficiently addressed, remedied, or protected Plaintiffs and Class members following the Data Breach and has taken adequate preventive and precautionary measures to ensure the Plaintiffs and Class members will not experience further harm;
- whether Plaintiffs and members of the Class suffered injury as a proximate result of Equifax's conduct or failure to act; and
- whether Plaintiffs and the Class are entitled to recover damages, equitable relief, and other relief, and the extend of the remedies that should be afforded to Plaintiff and the Class.

COUNT I

Negligence

(Individually and on Behalf of the Class)

40. Plaintiffs reallege and incorporates all previous allegations.
41. Equifax collected Confidential Information from Plaintiffs and Class Members.
42. Equifax owed a duty to Plaintiffs and the Class to maintain confidentiality and to

exercise reasonable care in safeguarding and protecting their financial and personal information in Equifax's possession from being compromised by unauthorized persons. This duty included, among other things, designing, maintaining, and testing Equifax's security systems to ensure that Plaintiffs' and Class members' financial and personal information in Equifax's possession was adequately protected.

43. Equifax further owed a duty to Plaintiffs and Class members to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

44. Equifax owed a duty to Plaintiffs and members of the Class to provide security consistent with industry standards and requirements, to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the financial and personal information of Plaintiffs and members of the Class whose confidential data Equifax obtained and maintained.

45. Equifax knew, or should have known, of the risks inherent in collecting and storing the financial and personal information of Plaintiffs and members of the Class and of the critical importance of providing adequate security of that information.

46. Equifax's conduct created a foreseeable risk of harm to Plaintiffs and members of the Class. This conduct included but was not limited to Equifax's failure to take the steps and opportunities to prevent and stop the data breach as described in this Complaint. Equifax's conduct also included its decision not to comply with industry standards for the safekeeping and maintenance of the financial and personal information of Plaintiffs and Class members.

47. Equifax acted with wanton disregard for the security of Plaintiffs and Class members' Confidential Information. Defendant knew or should have known that it had

inadequate computer systems and data security practices to safeguard such information, and Equifax knew or should have known that hackers were attempting to access the personal information in databases such as Equifax's.

48. Equifax breached the duties it owed to Plaintiffs and members of the Class by failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the medical, financial, and personal information of Plaintiff and members of the Class, as identified above. This breach was a proximate cause of injuries and damages suffered by Plaintiffs and Class members.

49. As a direct and proximate result of Equifax's negligent conduct, Plaintiffs and Class members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II
Negligence *Per Se*
(Individually and on behalf of the Class)

50. Plaintiffs reallege and incorporates all previous allegations.

51. Pursuant to the Federal Trade Commission Act (15 U.S.C. §45), Equifax had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' personal information.

52. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Equifax, of failing to use reasonable measures to protect Confidential Information.

53. Equifax violated § 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Confidential Information and not complying with applicable industry standards. Equifax's conduct was particularly unreasonable given the nature and amount of Confidential Information it obtained and stored and the foreseeable consequences of a data breach at a credit reporting company, including, specifically, the immense damages that would result to consumers and financial institutions.

54. The harm that has occurred is the type of harm the FTC Act (and similar state statutes) is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

55. Equifax had a duty to Plaintiffs and Class members to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class members' Confidential Information.

56. Equifax breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act (and similar state statutes), by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' financial and personal information.

57. Equifax's violation of §5 of the FTC Act (and similar state statutes) and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

58. But for Equifax's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

59. The injury and harm suffered by Plaintiffs and Class Members was the reasonably

foreseeable result of Equifax's breach of its duties. Equifax knew or should have known that it was failing to meet its duties, and that its breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Confidential Information.

60. As a direct and proximate result of Equifax's negligence per se, Plaintiffs and Class Members have suffered harm, including but not limited to loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the purchases made at Equifax that Plaintiffs and Class members would have never made had they known of Equifax's careless approach to cybersecurity; lost control over the value of personal information; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Card Information, entitling them to damages in an amount to be proven at trial.

COUNT III
UNJUST ENRICHMENT
(Individually and on Behalf of the Class)

61. Plaintiffs reallege and incorporates all previous allegations.

62. Plaintiffs and Class Members conferred a benefit upon Equifax in the form of consumers' information.

63. Equifax appreciated or had knowledge of the benefits conferred upon them by Plaintiffs and Class members. Equifax also benefited from the receipt of Plaintiffs' and Class members' Confidential Information, as this was utilized by Equifax to facilitate payment to it.

64. The monies that Equifax made by using Plaintiffs' and Class members' Confidential Information were supposed to be used by Equifax, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

65. Under principals of equity and good conscience, Equifax should not be permitted to retain the benefits gained from the use of Plaintiffs' and Class members' Confidential Information because Equifax's failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiffs and Class Members that were otherwise mandated federal, state and local laws, and industry standards.

66. Equifax should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class members all unlawful or inequitable proceeds received by it as a result of the conduct and data breach alleged herein.

COUNT IV

Violations of the Delaware Consumer Fraud Act, 6 Del. code § 2513, *ET SEQ.* (Individually and on Behalf of the Class)

67. Plaintiff Kuss realleges and incorporates by reference all paragraphs as though fully set forth herein.

68. The Delaware Consumer Fraud Act ("CFA") prohibits the "act, use or employment by any person of any deception, fraud, false pretense, false promise, misrepresentation, or the concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale, lease or advertisement of any merchandise, whether or not any person has in fact been misled, deceived or damaged thereby." 6 Del. Code § 2513(a).

69. Equifax is a person with the meaning of 6 Del. Code § 2511(7).

70. As described herein Equifax failed to adequately safeguard and protect

consumers' Confidential Information as alleged herein. Equifax knew of the breach and failed to adequately disclose the breach to affected consumers. Accordingly, Equifax engaged in unlawful trade practices, including by concealing and omitting material information from Plaintiff and the Class that there was a breach and that Equifax's cybersecurity was inadequate. Defendant engaged in deceptive business practices prohibited by the Delaware Consumer Fraud Act. Equifax's material omissions and misrepresentations were made with the intent that Plaintiff and the Class would rely upon them, and Plaintiff and the Class did in fact rely upon those material omissions and misstatements.

71. Equifax's actions as set forth above occurred in the conduct of trade or commerce.

72. Equifax's conduct proximately caused injuries to Plaintiff Kuss and the Class.

73. Plaintiff is entitled to recover damages, as well as costs and reasonable attorney fees as provided by the Delaware Consumer Fraud Act.

COUNT V
Violations of the Pennsylvania Unfair Trade Practices and
Consumer Protection Law, 73 Pa. C.S.A §§ 201-1, *et seq.* ("UTPCPL")
(Individually and on behalf of the Class)

74. Plaintiff Markowitz repeats, realleges, and incorporates by reference each of the foregoing factual allegations as though fully set forth herein.

75. Plaintiff Markowitz brings this claim on behalf of herself and the Class.

76. The UTPCPL makes unlawful "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce."

77. The UTPCPL provides a private right of action for any person who "suffers any ascertainable loss of money or property, real or personal, as a result of the use or employment by any person of a method, act or practice declared unlawful by" the act. 73 Pa. C.S.A. § 201-9.2(a).

78. The UTPCPL applies to the claims of Plaintiff and the Class because the conduct by Defendant alleged herein which constitutes violation of the UTPCPL by Defendants occurred in substantial part within the Commonwealth of Pennsylvania.

79. Plaintiff Markowitz and the Class are consumers whose information was collected by Defendant and compromised while in Defendant's possession. Defendant's services are primarily for personal, family or household purposes within the meaning of 73 Pa. C.S.A. § 201-9.2.

80. Defendant used and employed unfair or deceptive acts or practices within the meaning of 73 Pa. C.S.A. §§ 201-2 and 201-3 by inadequately protecting consumers' Confidential information and by failing to timely notify affected consumers of the Data Breach.

81. Plaintiff Markowitz and Class members relied upon Defendant's representations and omissions that their Confidential Information would be adequately protected in Defendant's possession.

82. As a direct and proximate result of Defendant's violations of the UTPCPL, Plaintiff Markowitz and Class members have suffered an ascertainable loss of money and will continue to suffer a loss of money and are therefore entitled to relief, including trebled damages, costs and attorneys' fees under Section 201-9.2 of the UTPCPL.

PRAYER FOR RELIEF

Plaintiffs, on behalf of themselves and the Class, respectfully requests that the Court grant the following relief:

A. Certify this case as a class action pursuant to FED. R. CIV. P. 23(a) and (b)(3), and, pursuant to FED. R. CIV. P. 23(g), appoint Plaintiffs as Class representatives and their counsel as Class counsel.

B. Award Plaintiffs and the Class appropriate monetary relief, including actual damages, restitution, and disgorgement.

C. Award Plaintiffs and the Class equitable, injunctive and declaratory relief as may be appropriate. Plaintiffs, on behalf of the Class, seek appropriate injunctive relief designed to ensure against the recurrence of a data breach by adopting and implementing best security data practices to safeguard customers' financial and personal information and extend credit monitoring services and services to protect against all types of identity theft, especially including card theft, credit reports, and fraudulent card charges, and to provide elevated credit monitoring services to minor and elderly Class members who are more susceptible to fraud and identity theft.

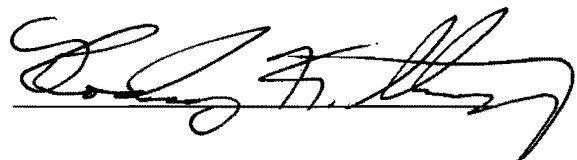
D. Award Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable.

E. Award Plaintiffs and the Class reasonable attorneys' fees and costs as allowable.

F. Award Plaintiffs and the Class such other favorable relief as allowable under law or at equity.

Dated: September 8, 2017

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Rodney K. Strong", written over a horizontal line.

Griffin & Strong, P.C.

Rodney K. Strong
GA Bar No. 688730

GA Bar No. 688730
David J. Maher
GA Bar No. 485370
235 Peachtree Street, N.E.
Suite 400
Atlanta, Georgia 30303
(404)-584-9777 (phone)
(678)-960-7861 (fax)
Email: Rodney@gspclaw.com
david@gspclaw.com

CHIMICLES & TIKELLIS LLP
PA ID No. 50579
Benjamin F. Johns
PA ID No 201373
One Haverford Centre
361 West Lancaster Avenue
Haverford, PA 19041
Telephone: (610) 642-8500
Facsimile: (610) 649-3633
E-mail: SAS@chimicles.com
BFJ@chimicles.com